

Preface

The information infrastructure – comprising computers, embedded devices, networks and software systems – is vital to operations in every sector: chemicals, commercial facilities, communications, critical manufacturing, dams, defense industrial base, emergency services, energy, financial services, food and agriculture, government facilities, healthcare and public health, information technology, nuclear reactors, materials and waste, transportation systems, and water and wastewater systems. Global business and industry, governments, indeed society itself, cannot function if major components of the critical information infrastructure are degraded, disabled or destroyed.

This book, *Critical Infrastructure Protection XI*, is the eleventh volume in the annual series produced by IFIP Working Group 11.10 on Critical Infrastructure Protection, an active international community of scientists, engineers, practitioners and policy makers dedicated to advancing research, development and implementation efforts related to critical infrastructure protection. The book presents original research results and innovative applications in the area of infrastructure protection. Also, it highlights the importance of weaving science, technology and policy in crafting sophisticated, yet practical, solutions that will help secure information, computer and network assets in the various critical infrastructure sectors.

This volume contains sixteen revised and edited papers from the Eleventh Annual IFIP Working Group 11.10 International Conference on Critical Infrastructure Protection, held at SRI International in Arlington, Virginia, USA on March 13–15, 2017. The papers were refereed by members of IFIP Working Group 11.10 and other internationally-recognized experts in critical infrastructure protection. The post-conference manuscripts submitted by the authors were rewritten to accommodate the suggestions provided by the conference attendees. They were subsequently revised by the editors to produce the final chapters published in this volume.

The chapters are organized into four sections: (i) infrastructure protection; (ii) infrastructure modeling and simulation; (iii) industrial control system security; and (iv) Internet of Things security. The coverage of topics showcases the richness and vitality of the discipline, and offers promising avenues for future research in critical infrastructure protection.

This book is the result of the combined efforts of several individuals and organizations. In particular, we thank David Balenson, Molly Keane and Zachary Tudor for their tireless work on behalf of IFIP Working Group 11.10. We gratefully acknowledge Idaho National Laboratory and the Institute for Information Infrastructure Protection (I3P), managed by George Washington University, for their sponsorship of IFIP Working Group 11.10. We also thank the U.S. Department of Homeland Security, National Security Agency and SRI International for their support of IFIP Working Group 11.10 and its activities. Finally, we wish to note that all opinions, findings, conclusions and recommendations in the chapters of this book are those of the authors and do not necessarily reflect the views of their employers or funding agencies.

MASON RICE AND SUJEET SHENOI

Critical Infrastructure Protection XI

11th IFIP WG 11.10 International Conference, ICCIP

2017, Arlington, VA, USA, March 13-15, 2017, Revised

Selected Papers

Rice, M.; Shenoi, S. (Eds.)

2017, XVI, 338 p. 116 illus., Hardcover

ISBN: 978-3-319-70394-7